

# Reliability Practice at NASA Goddard Space Flight Center

Ming Li, PhD, Mantech SRS

Paula S. Pruessner, NASA Goddard Space Flight Center

Key Words: Reliability, NASA

## SUMMARY AND CONCLUSION

*This paper describes in brief the Reliability and Maintainability (R&M) Programs performed directly by the reliability branch at Goddard Space Flight Center (GSFC). The mission assurance requirements flow down is explained. GSFC practices for PRA, reliability prediction/fault tree analysis/reliability block diagram, FMEA, part stress and derating analysis, worst case analysis, trend analysis, limit life items are presented. Lesson learned are summarized and recommendations on improvement are identified.*

## 1 INTRODUCTION

The Goddard Space Flight Center (GSFC) is a major U.S. laboratory for developing and operating unmanned scientific spacecraft. GSFC manages many of NASA's Earth Observation, Astronomy, and Space Physics missions, such as Landsat, Geostationary Operational Environmental Satellite (GOES), and the James Webb Space Telescope (JWST). The implementation of Reliability and Maintainability Programs at GSFC assure that safe, reliable, and high-quality systems are delivered.

This paper summarizes the Reliability and Maintainability (R&M) practices conducted by the reliability branch at NASA GSFC. Section 2 describes the NASA reliability policies and standards on mission assurance and the flow down of NASA policies and standards to related Goddard Mission Assurance Requirements documentation. Section 3 introduces select R&M activities at GSFC, including the values added to the mission by applying R&M activities and some real examples.

## 2 NASA R&M POLICIES

The NASA Policy Directives (NPD) 1000.0 [1], which sets forth the principles and identifies the specific requirements for NASA strategic management, specifies that "NASA employs a system of checks and balances for effective internal control and to ensure the successful achievement of missions, assigning proper levels of influence and action to different organizations. Program and project management focuses upon execution. Engineering maintains independent authority by setting technical requirements below the Directorate-owned top-level requirements and approving any

deviation from such requirements. The Safety & Mission Assurance organization maintains responsibility for verification of programmatic compliance through strategies, policies, and standards. Mission Support offices also provide institutional checks and balances." (NASA NPD 1000.0 Section 3.2.5) The Office of Safety and Mission Assurance (OSMA) "provides policy direction, functional oversight, and assessment for all Agency safety, reliability, maintainability, and quality engineering and assurance activities and serves as a principal advisory resource for the Administrator and other senior officials on matters pertaining to safety and mission success."

The NPD 8700.1 [2] further defines the NASA policy for safety and mission success as to "Protect the public, Astronauts and pilots, NASA workforce, and high-value equipment and property from potential harm", to "establish and maintain independent lines of communications for unrestricted flow of information concerning Safety and Mission Assurance (SMA), risks, or other matters affecting the ability to meet the mission-success criteria", to "define and document both SMA requirements and safety and mission success criteria", to "Verify and validate life-cycle implementation of SMA, RM, and success requirements".

The NPD 8720.1 [3] refines the NASA R&M policy as

- "Establish, document, and implement
  - (1) System R&M design and operational performance requirements (qualitative and quantitative).
  - (2) System maintenance concepts, including, but not limited to, maintenance requirements, schedule, and responsibilities.
  - (3) R&M engineering, analysis, testing, and maintenance activities addressing hardware, software, firmware, and human elements.
  - (4) Timely and continuous assessment of compliance with the R&M requirements and the continuous identification of areas for improvement.
  - (5) Integration of R&M engineering activities with systems engineering, risk management, and other processes, assessments, and analyses including, but not limited to, safety, security, quality assurance, logistics, probabilistic risk assessment, life-cycle cost, configuration management, and maintenance.

- Share R&M data and experience for use as heritage data in support of current, follow-on, and new programs or projects.”

The NASA Standard 8729.1 [4] for R&M provides “provides guidance to customers (or purchasers) and suppliers (or contractors) on R&M requirements development, design implementation, and evaluation.”

Figure 1 depicts the NASA Safety and Mission Assurance Requirements Tree as described above.

At Goddard, the program functional and performance requirements, including the mission assurance requirements such as reliability, maintainability and availability (RMA), are summarized in level I requirements documents. Such RMA requirements conform to the NASA Mission Assurance policies and standards. The level I requirements then flow down to the project requirements as the so called Mission Assurance Requirements (MAR) document. This paper summarizes R&M activities specified in this document.

### 3 GSFC R&M ACTIVITIES AND EXAMPLES

The Mission Assurance Requirements document compiles NASA quality, safety, reliability and maintainability requirements. The Reliability Program Plan (RPP, also termed Reliability, Maintainability and Availability Program Plan in some circumstances) provides planning and control for the reliability and maintainability programs based upon the MAR. This section describes the representative reliability tasks presented in MAR.

In general, the reliability discipline shall plan and implement a reliability program that interacts effectively with other project disciplines, including systems engineering, hardware design, and product assurance. The program shall be tailored to:

- Assure the specified reliability probability of success is achieved.
- Demonstrate that redundant functions, including alternative paths and work-arounds, are independent to the extent practicable
- Demonstrate that the stress applied to parts meet applicable derating criteria.
- Identify single failure items/points, their effect on the attainment of mission objectives, and possible safety degradation.
- Identify limited-life items and ensure that special precautions are taken to conserve their useful life for on-orbit operations.

The GSFC reliability branch primary focus is on the following reliability analyses: PRA, parts stress and derating, reliability prediction, fault tree analysis, FMEA. This paper will focus on the same. Worst case analysis, trend analysis and limited life items are generally performed by the design engineer with assistance of the reliability engineer and are under reliability branch review. These topics will not be covered in detail in this paper.

#### 3.1 Probabilistic Risk Assessment (PRA)

PRA is a scenario based analysis used to assess the probability of failure (risk) or success of a system's operation [5] [6]. Results provided by this risk assessment methodology are used to make decisions concerning choices of improvements to the design and operation. NASA PRA is defined in the NPR 8705.5 as a ten step process.

GSFC practices PRA as defined in 8705.5. A number of limited scope or simplified PRAs have been conducted recently for the IBEX, LRO, and MMS missions. “Limited scope” entails an analysis performed only on certain phases, levels, or end states of interest. In some cases, the analysis is simplified by not including uncertainty analysis due to the lack of uncertainty data. An ongoing NASA inter-center effort is aimed at establishing a PRA database to advance the PRA practice at GSFC and other NASA centers.

Both the IBEX and LRO PRAs identified critical mission failures scenarios. The scenarios were used by the systems engineers to understand the possible failures and potential mitigations. In addition, the LRO PRA estimated the failure probability of the LRO minimum mission.

#### 3.2 FMEA

Failure Modes and Effects Analysis (FMEA) is a systematic method of identifying and classifying product and process problems before they occur [7][8]. The FMEA process is part of a quality system focused on preventing defects, improving reliability, enhancing safety, and increasing customer satisfaction. The analysis is used as a “bottoms-up” approach to assess high risk items and the activities underway to provide corrective actions. FMEA is also used to define special test considerations, quality inspection points, operational constraints, and activities necessary to minimize failure risk. The objective of a FMEA is to look for all of the ways a process or product can fail and what the effect of this failure would be on different levels of the system. The FMEA determines the effect of each failure on system operation and identifies single point failures, which are critical to mission success.

To be effective, FMEAs should be performed as early in the design process as possible. MIL-STD-1629 states that the FMEA should be initiated as soon as preliminary design information is available at the higher system levels and extended to the lower levels as more information becomes available on the items in question. The emphasis on an early FMEA development ensures that issues are discovered and corrected as early in the design process as possible, before expensive redesign becomes necessary. Generally, a functional FMEA is done early in the life cycle, and revised with more details as the design is firmed up. Interface FMEAs are performed on all interfaces with ground equipment or spacecraft to hardware to ensure no damage will occur in the event of failures.

Table 1 presents the failure mode severity categories used in GSFC.

There are a number of areas where GSFC is working with

contractors to improve FMEA practices to provide better information to projects.

1. For redundant components, some FMEAs have assumed one component fails and redundancy takes over and concludes that there are no effects to the system. Based upon MIL-STD-1629A, the better approach assumes both primary and redundant components fail at the same time and then investigate its effect to the system. More emphasis is being placed now on common cause failures.
2. Software is often minimally covered in FMEAs, if at all. While critical software that acts as a control is covered through safety hazard analyses, there is still improvement needed in the way software is examined. For software failures, both the software response to the hardware failures (from software input side) and failures caused by software itself should be considered in the FMEA. This subject is currently being improved through work with NASA headquarters.
3. Process FMEAs, which are a useful tool to analyze facilities to minimize safety hazards, mitigate operations risks, and improve handling processes, are not fully utilized to the extent feasible.
4. The NASA method of separating criticality 1 items into 1, 1S, and 1R and criticality 2 items into 2 and 2R can lead to an improper categorization of failure modes, such as minimizing the risk of "critical" redundant items to "minor" criticalities. MIL-STD-1629A has four categories and would work better.

GSFC is currently working on an FMEA standard that will take some of these lessons learned into account, in an effort to improve the FMEA practice.

### 3.3 Worst Case Analysis (WCA)

The WCA examines the possible worst situation that may apply to the critical mission components (FMEA category 1 and 2) and demonstrates the adequacy of margin in the design of electronic and electrical circuits, optics, and electromechanical and mechanical items. This analysis was normally completed by design engineer and reviewed by reliability engineer at GSFC.

### 3.4 Trend Analysis

Trend Analysis monitors parameters on assemblies and subsystems throughout the normal test program that relate to performance stability (any deviations from the nominal that could indicate trends), and coordinates results with design and operational personnel. The Integration & Test (I&T) engineer normally performs this analysis at GSFC.

### 3.5 Limited Life Items

The Limited Life Items defines and tracks the selection, use and wear of limited-life items, such as fuel and propellant, and the impact on mission operations. Limited-life items consider the affects of atomic oxygen, solar radiation, shelf-life, extreme temperatures, thermal cycling, wear and fatigue; mechanisms such as seals, bearings, valves, actuators and scan

devices when aging, wear, fatigue and lubricant degradation limit their life are examined.

### 3.6 Part Stress and Derating Analysis

Part Stress and Derating Analysis examines the operational stress margins for the parts. Each application of electrical, electronic, and electromechanical (EEE) parts shall be subjected to stress analyses for conformance with the applicable derating guidelines. The analyses shall be performed at the most stressful values that result from specified performance and environmental requirements (e.g., temperature and voltage) on the assembly or part. GSFC uses INST-EEE-002 [9] as the part stress and derating standard.

Part stress and derating analysis is a preventive approach and should be performed before parts are procured. Some failures can be screened and prevented during design process. In one incident, two 12V rated capacitors were misused in 18V circuitry and were not screened by proper part stress and derating analysis. The two capacitors exploded after the circuitry was powered on and damaged the board. Measures are being taken to prevent such incidences from occurring in the future.

### 3.7 Reliability Prediction / Fault Tree Analysis / Reliability Block Diagram

The GSFC reliability prediction models/estimates system or mission reliability utilizing reliability block diagram (RBD) and fault tree (FT). The RBD and FT analyses normally remains at the component (card) level but may vary to accommodate the failure rate availability at a higher level (such as the failure rate of a gyro may be available from heritage data); or address the need to model the lower level redundancy or critical component (such as sub-card level redundancy or a switch which controls the redundant cards)

The key to the success of reliability prediction is to obtain the basic event failure rates. GSFC utilizes the following sources of failure data: performance of similar elements (heritage data), test data, handbook data (MIL-HDBK-217F, failure rates from the Reliability Information Analysis Center (RIAC), or equivalent). Due to the unique nature of NASA space missions (almost every system is the prototype of its kind, and failed items are not available for examination, although the telemetry data can provide limited diagnostic information), heritage data and test data are not always available. GSFC reliability prediction often depends heavily on the use of handbook failure data, especially MIL-HDBK-217F2 data [10].

The MIL-HDBK-217F2 defines two methods, namely "part stress analysis" and "parts count", to estimate the failure rate of an individual part and calculate the failure rate of a card by summing up failure rates of all parts in that card (any in-card redundancy should be modeled in the FT).

The "part stress analysis" method assumes a base failure rate for the part and then correlates the failure rate with part's functional characteristics, quality level and stresses applied. Stresses includes electrical (current, voltage, etc) and environmental stresses (e.g. temperature, operational

environment such as ground, space). This method requires detailed information and is applicable during the later design phase when actual hardware and circuits designs are available.

The "parts count" method determines the part failure rate based upon the base failure rate, the quality level of the part, and the application environment. The component failure rate is the sum of all part failure rates. This method is applicable during the early design phase and during proposal formulation.

Temperature is one of the major factors that influence EEE (Electrical, Electronic, and Electromechanical) part failure rate. GSFC practices show that, in general, every 10 °C temperature increase doubles the failure rate. The failure rate used in "parts count" method is roughly equivalent to the failure rate calculated using "part stress analysis" at the temperature of 25 °C. Therefore if the operation temperature is warmer than this, one would consider using "part stress analysis" method as a more credible prediction.

Although it is used readily in reliability analyses, MIL-HBK-217F2 has not been updated since 1995 and failure rates are considered to be conservative for space systems. Thus, the use of MIL-HBK-217 in reliability prediction is most valuable when used to compare different designs (trade study) and identify weak links in the design, rather than to demonstrate reliability of the mission. Actual field data is always preferred, but not always available. Physics of failure models can be used to perform trade studies and predict on-orbit performance. GSFC is currently studying various standards (i.e. 217 Plus, Telcordia, etc.) to choose a standard for use when more applicable data is not available.

One area in which reliability prediction has been of great use is at the early conceptual design stage at the Goddard Integrated Mission Design Center. In these efforts, conceptual designs of potential Goddard missions are evaluated to 1) verify the reliability targets can be satisfied; 2) identify the weak links of the design and propose the corresponding mitigation (more redundancy and or more reliable parts); 3) trade different designs as one of the major selection criteria.

Although it can be difficult to get good information on failures occurring once satellites are on orbit, heritage data is also used to update reliability predictions when insight is needed on how a system will operate in a space environment. On GLAST, a reaction wheel failure during testing concerned the program. Performing a Weibull analysis on all similar reaction wheels that had flown or were in operation allowed GSFC to bound and accept the risk presented by this issue.

#### *SUMMARY RECOMMENDATIONS AND CONCLUSIONS*

GSFC R&M provides planning, analysis, and surveillance support and consultation in the areas of reliability, maintainability, availability, risk assessment, and mission success throughout all phases (i.e., proposal, design, build, integration, test, and operations) for space system architecture & operations development, and execution.

GSFC continues to provide excellent R&M services in support of space missions. Improvements continue to be discussed and planned in the following areas:

1. Collaborations with other NASA centers for better, more applicable failure data.
2. Increased involvement at the early stage in the life cycle.
3. More profound use of PRA during the life cycle.
4. Better incorporation of software reliability and maintainability.

As R&M techniques are further refined and better data is collected to more accurately predict mission lifetimes, reliability support will continue to be of great use to GSFC missions.

#### *REFERENCES:*

1. NASA Strategic Management and Governance Handbook, NASA Policy Directives 1000.0, August 2005, Washington DC
2. NASA Policy for Safety and Mission Success, NASA Policy Directives 8700.1C, October 2002, Washington DC
3. NASA Reliability and Maintainability (R&M) Program Policy, NASA Policy Directives 8720.1C, April 2008, Washington DC
4. Planning, Developing and Managing an Effective Reliability and Maintainability (R&M) Program, NASA STD 8729.1, December 1998, Washington DC
5. Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects, NASA Procedural Requirements 8705.5, July 2004, Washington DC
6. H. Kumamoto, E. Henley, Probabilistic Risk Assessment and Management for Engineers and Scientists, 2<sup>nd</sup> edition, IEEE Press, New York, 1996
7. Procedures for Performing a Failure Mode Effects and Criticality Analysis, Military Standard, MIL-STD-1629A, November 1980, Washington DC
8. Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA), International Standard, IEC 60812, Switzerland, 2006
9. K. Sahu, Instructions for EEE Parts Selection, Screening, Qualification, and Derating, EEE-INST-002, NASA Goddard Space Flight Center, May 2003, Greenbelt, MD
10. Reliability Prediction of Electronic Equipment, Military Handbook, MIL-HDBK-217F Notice 2, 1995, Washington DC

#### *BIOGRAPHIES*

Ming Li, PhD  
NASA Goddard Space Flight Center / SRS Technologies  
Mail Stop 300.1,  
Greenbelt, MD 20771

Email: Ming.Li@ieee.org

Ming Li serves as a Senior Reliability Engineer contractor at NASA Goddard Space Flight Center for ManTech SRS Technologies in

Greenbelt, Maryland. His field of interest is in software reliability assessment, system reliability modeling and PRA for complex systems. He received his B.S. in EE and M.S. in Systems Engineering from Tsinghua University, China, and Ph.D in Reliability Engineering from the University of Maryland, College Park. He has authored over 27 papers in peer reviewed journals and international conferences.

Paula S. Pruessner, CRE  
NASA Goddard Space Flight Center,  
Code 322  
Greenbelt, MD 20771

Email: Paula.S.Pruessner@nasa.gov

Paula S. Pruessner is a senior reliability engineer at NASA, Goddard Space Flight Center (GSFC), in Greenbelt, Maryland. She is the project reliability manager on the LDCM and GOES-R missions. Ms. Pruessner received her M.S. in Reliability Engineering in 2003 and B.S. in Mechanical Engineering in 2000 from University of Maryland in College Park. She is an ASQ Certified Reliability Engineer. Her professional interests include system reliability modeling and risk analysis.

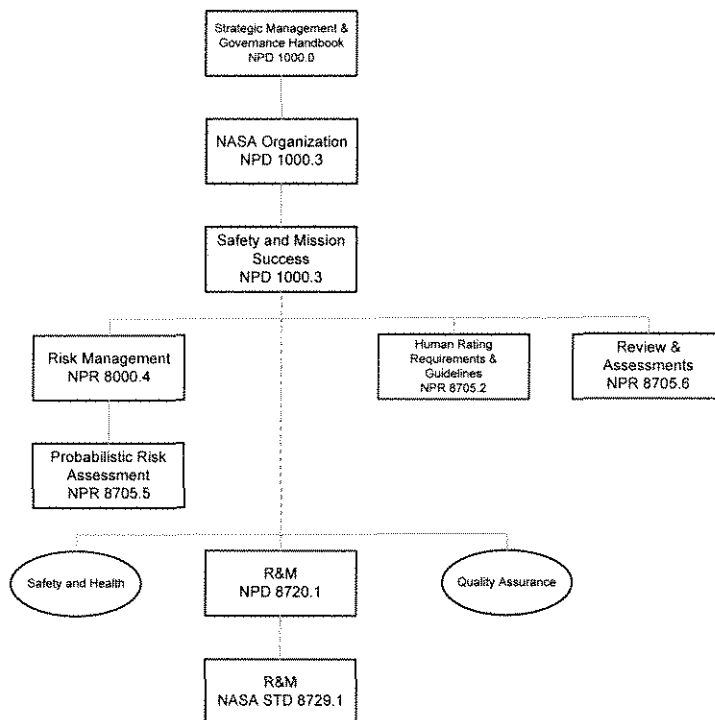


Figure 1 NASA Safety and Mission Assurance Requirements Tree

*Table 1 FMEA Severity Category*

Severity Categories Table

Category	Severity	Description
1	Catastrophic	Failure modes that could result in serious injury, loss of life, or loss of a satellite, or launch vehicle.
1R		Failure modes of identical or equivalent redundant hardware items that, if all failed, could result in category 1 effects.
1S		Failure in a safety or hazard monitoring system that could cause the system to fail to detect a hazardous condition or fail to operate during such condition and lead to Severity Category 1 consequences.
2	Critical	Failure modes that could result in loss of one or more mission objectives as defined by the GOES R Project office.
2R		Failure modes of identical or equivalent redundant hardware items that could result in Category 2 effects if all failed.
3	Significant	Failure modes that could cause degradation to mission objectives.
4	Minor	Failure modes that could result in insignificant or no loss to mission objectives